## REMARKS/ARGUMENTS

We have canceled claims 1-8, 33-38, 60, 65, and 68. We have also amended claim 59 to include the limitation of claim 60 relating to offsets. After entering the proposed amendments, claims 9-32, 39-59, 61-64, 66, 67, and 69-71 will be pending in this application.

The examiner rejected claims 1-71 under 35 U.S.C. §103(a) as being unpatentable over U.S. 5,465,084 to Cottrell. The examiner admits that Cottrell does not teach "error-correcting" in the sense of the claims. But he argues:

> Nevertheless, it is well known in the art to have a [sic] "error-correcting" situation in computer entry for the motivation of permitting ease of entry of data (by permitting a reasonable amount of error in entry)
>
> Hence, it would have been obvious to those of ordinary skill in the art at the time of the claim invention to modify Cottrell for the motivation noted in the previous paragraphs so as to teach the claimed invention.

However, even if we assume that the use of error correcting codes in general were well known in the art at the time of this invention, that does not render obvious the particular way in which the error correcting codes are used in the present inventions. The examiner has, in fact, provided no support whatsoever for concluding that the particular way in which error codes are used in the present inventions were obvious or known. He has identified no prior art to support his position. He has only made a general observation that "it is well known in the art to have a [sic] 'error-correcting' situation in computer entry for the motivation of permitting ease of entry of data."

Moreover, the examiner has not explained how Cottrell would work if "error-correcting" codes were used. He has simply asserted that it would be obvious to modify Cottrell to use error-correcting codes. In Cottrell's system, what is the uncertainty that the error correcting code would be correcting for? There is no hint in Cottrell that uncertainty might be a problem or that it might be useful to modify the code to accommodate any uncertainty in the input pattern.

It is worth examining more closely how Cottrell's system operates. This is what Cottrell says:

> In order to understand the concept...the password is merely a pre-selected two or three dimensional pattern of elements represented by symbols and/or colors, each of which can be represented by a unique computer code. For instance, the standard ASCII code translates 256 European language alphanumerics and symbols into a one-byte computer code...A person wishing to obtain access to the protected device merely describes the pattern by some means available to that person and also recognizable by the security device so the security device can compare the pattern of symbols and/or colors (the "password") presented by the person seeking access and the permitted patterns on a position-and-symbol to position-and-symbol basis and without regard to the sequence in which the elements (e.g. symbols and/or colors) constituting the pattern are entered. The patterns are compared and if the pattern presented matches one of the authorized patterns, the device grants access to the requestor. A simple 10 x 10 grid in which a password pattern of any size is entered produces a device which has a chance of a random match of one in $6.6 \times 10^{240}$ if only the standard 256 ASCII characters are used. It is virtually impossible to obtain a match to the pattern through a random guess, even with the fastest supercomputer. (Col. 2,line 55 to col. 3, line 19).

It is noteworthy that Cottrell computes the probability of a random match occurring. His computed number assumes that no error correcting code is used; it assumes an exact match must occur, namely, the precise sequence of ASCII characters placed into the correct arrangement 2-dimensional pattern within a 10 x 10 grid. Cottrell seems to be advocating one of the strengths of his system, which is the low probability for guessing the visual password. Incorporating an error correcting code would undoubtedly increase the probability of a random match occurring.

But in view of how Cottrell's system operates, how might an error correcting code be used in Cottrell? One can imagine that some leeway might be permitted in either the character that is placed into the required grid position or in the grid position that is assigned to that character. But in either case, the resulting system is not what is claimed.

The claims recite a specific way in which the input pattern is processed. For example, in claim 9 each discrete graphical choice of a sequence of discrete graphical choices that is entered by the user is first converted into a corresponding value to produce a sequence of values. Cottrell does not even suggest such a conversion. Contrary to what the examiner appears to believe, Cottrell does not suggest that his input pattern is converted to a sequence of values. The examiner pointed to col. 2, lines 10-45 as teaching this concept; but we could find nothing in that part of Cottrell's disclosure or any other part of Cottrell's disclosure for that matter which taught this concept.

But claim 9 requires more than that. Claim 9 also recites the following two additional steps:

> for the sequence of values selecting codewords from a plurality of codewords to generate a sequence of codewords, the plurality of codewords being associated with an error-correcting code;
>
> calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets

The examiner has not explained how such a mapping of the elements of Cottrell's input pattern to a corresponding sequence of codewords selected from an error correcting code might be performed in Cottrell's system. He has pointed to no prior art that suggests how it might be performed. And in the case of the offset, the examiner appears to simply have ignored this aspect of the invention. He has not identified where Cottrell or anybody else for that matter teaches computing offsets of any kind. Moreover, we could find no teaching by Cottrell of the use of offsets. Indeed, we could not even find mention of the word "offset" anywhere in Cottrell.

For at least the reasons presented above, we submit that claim 9 is allowable over the art of record.

In the case of the other pending independent claims, each one makes a reference to either computing or using offsets. The relevant portions of the claims are as follows:

Claim 20: retrieving a sequence of offsets

Claim 39: an offset calculator in signal communication with the codeword generator, the offset calculator calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets

Claim 48: a memory element in signal communication with a summer, the memory element containing a sequence of offsets; the summer in signal communication with the converter and the memory element, the summer summing each input value from the sequence of input values with the corresponding offset from the sequence of offsets to generate a sequence of intermediate values

Claim 59: calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets for use in re-generating the secret

For at least that reason, we submit that all of the other independent claims (as well as the claims dependent therefrom) are also allowable over the art of record.

Please apply any charges not covered, or any credits, to Deposit Account No. 08-0219.

Respectfully submitted,

Date: September 20, 2005

Eric L. Prahl
Reg. No. 32,590

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, MA 02109
Telephone: (617) 526-6000
Facsimile: (617) 526-5000